e-LAWTREND

№ 1

январь - апрель 2013г.

СВОБОДА ИНТЕРНЕТА В БЕЛАРУСИ

Обзор законодательства и практики

ЦЕНТР ПРАВОВОЙ ТРАНСФОРМАЦИИ
220052, Беларусь, Минск, ул. Нововиленская, 38. +375 17 335 44 86 info@lawtrend.org
www.lawtrend.org www.fb.com/lawtrend

АНАЛИЗ ПРОЕКТА НОВОЙ РЕДАКЦИИ ЗАКОНА «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ»*: РАБОТА НАД ОШИБКАМИ?

В начале 2013 года стало известно, что Палата Представителей Национального собрания Республики Беларусь ведет работу над проектом закона «О внесении изменений и дополнений в Закон Республики Беларусь «Об информации, информатизации и защите информации» (далее - Закон). Текст проекта Закона доступен для ознакомления общественности на национальном правовом портале Республики Беларусь.

Закон «Об информации, информатизации и защите информации» регулирует важнейшие для информационного общества области: доступ к информации, в том числе к находящейся в распоряжении государства общественно значимой информации, и защиту информации (государственной тайны и других видов тайны, в том числе персональных данных).

Почему же Закон, принятый относительно недавно, в 2008 году, потребовал столь скорого пересмотра? Устраняет ли предложенный проект недостатки и пробелы текущего законодательства? Насколько существенные изменения предлагаются? Станет ли информация о деятельности государственных органов доступнее, а деятельность государственных органов более транспарентной? Получат ли защиту персональные данные граждан?

Эксперты Lawtrend проанализировали доступный общественности проект Закона: на что направлены изменения и в каком объеме предлагаются.

Сфера регулирования

Следует отметить, что Закон направлен на регулирование широкого круга общественных отношений в информационной сфере, связанных с поиском, получением, пользованием, передачей, сбором, обработкой, накоплением, хранением, распространением и предоставлением информации. С развитием разнообразных сервисов электронного правительства, коммерческих онлайн-сервисов граждане все чаще вступают в различные информационные отношения, например, заполняя онлайн-формы и оставляя свои данные при приобретении товара, производя поиск и сбор информации о потенциальных клиентах, направляя запросы в органы государственного управления для получения информации, находящейся в распоряжении государства. В каждом из этих случаев граждане тем или иным образом соприкасаются с информацией, а значит, находятся в поле действия Закона.

В такой ситуации для государства принципиально важно надлежащим образом обеспечивать реализацию двух важнейших для информационной сферы конституционных прав: **права на доступ к информации** (ст. 34 Конституции) и ***права на неприкосновенность частной жизни*** (ст. 28 Конституции). Они относятся к основополагающим правам человека и закреплены в базовых документах универсального характера (статья 12 и статья 19 Всеобщей декларации прав человека, статья 17 и статья 19 Международного Пакта о гражданских и политических правах).

Закон призван обеспечить реализацию указанных конституционных прав: право на информацию прямо зафиксировано в ст. 6 Закона, а право на неприкосновенность частной жизни получило реализацию через закрепление принципа защиты информации о частной жизни физического лица и его персональных данных как одного из принципов правового регулирования информационных отношений (ст. 4) и регламентации правовой защиты персональных данных (ст. 18).

Именно фиксация в Законе важнейших для информационного общества конституционных прав требует повышенного внимания к обсуждению Закона и тщательного анализа предлагаемых изменений.

*** по состоянию на 30 апреля 2013 года.**

Действующая редакция

Неудивительно, что Закон, принятый в 2008 году, потребовал скорого пересмотра: стремительное развитие информационно-коммуникационных технологий (ИКТ) требует адаптации законодательных подходов к новым «цифровым» **условиям**.

Более того, в действующей редакции Закона были выявлены существенные недостатки. Эксперты Lawtrend уже обращались к сфере регулирования Закона. Были отмечены некоторые недостатки и пробелы беларусского законодательства **в области реализации права на неприкосновенность частной жизни** и в части **обеспечения права на доступ к информации.**

В частности, ставится под сомнение целесообразность объединения вопросов доступа к информации и защиты персональных данных в одном законе. В нынешнем законодательстве отсутствует четкое определение информации, относящейся к частной жизни и персональных данных, не выделяются особо чувствительные категории информации, например, медицинские данные, и как следствие - отсутствует их адекватная защита. Критикуется также игнорирование Беларусью международных стандартов и наилучших практик в области защиты персональных данных, подлежащих автоматизированной обработке и, в частности, невосприятие на национальном уровне стандартов Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. На настоящий момент присоединение Республики Беларусь к Конвенции невозможно в связи с тем, что Республика Беларусь не является членом Совета Европы.

Именно поэтому, по мнению экспертов, предыдущая редакция Закона требует доработки и устранения недостатков. В связи с этим становится актуальным вопрос: устранит ли новая редакция существующие недостатки?

Право на доступ к информации

В проекте Закона закреплена возможность направления электронного запроса для предоставления общедоступной информации (ст. 21). Сложно назвать это серьёзным новшеством, скорее упорядочиванием норм в рамках единого нормативно-правового акта, регулирующего общественные отношения в сфере информации, так как такая возможность уже фиксировалась в Законе Республики Беларусь «Об обращениях граждан и юридических лиц».

Служебная информация ограниченного распространения

В то время как список общедоступной информации остался неизменен, добавлены новые категории информации, распространение и (или) предоставление которой ограничено **- служебная информация ограниченного распространения.**

Закон дополнен новой статьёй 181, которая определяет служебную информацию ограниченного распространения как «сведения, касающиеся деятельности государственного органа, иного юридического лица, распространение и (или) предоставление которых может причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц, и которые не отнесены к государственным секретам».

Перечни сведений информации ограниченного распространения формируются на основании решения руководителя государственного органа или иного юридического лица.

Дополнительные основания для отказа в предоставлении информации

2

В статье 21 появились дополнительные основания для отказа в предоставлении информации. Например, общедоступная информация может не предоставляться по запросу в случаях, если:

- в запросе ставится вопрос о выработке правовой позиции по запросу, проведении анализа деятельности государственного органа или проведении иной аналитической работы, непосредственно не связанной с защитой прав и законных интересов лица, направившего запрос;

- запрашиваемая информация опубликована в официальных периодических печатных изданиях, средствах массовой информации или размещена в открытом доступе в глобальной компьютерной сети Интернет.

При этом, Закон не обязывает государственный орган давать ссылку на такую информацию при формулировании отказа.

В случае, если "запрашиваемой информацией являются докладные, служебные записки, поручения должностных лиц и иная внутренняя переписка государственного органа, иного юридического лица, а также переписка между государственными органами, иными юридическими лицами, непосредственно не связанные с защитой прав и законных интересов лица, направившего запрос", организация также вправе отказать в предоставлении информации.

Доступ к информации на официальных сайтах

3

Проектом впервые на законодательном уровне устанавливается норма о том, что распространение и (или) предоставление общедоступной информации государственным органом может осуществляться в том числе и путём её размещения на официальных сайтах государственных органов в Интернете. Проект предусматривает внесение в закон положений о перечне информации, которые государственные органы обязаны размещать на своих интернет-сайтах.

Важным нововведением является норма об обязательном размещении республиканскими органами государственного управления, подчиненными Правительству Республики Беларусь, местными исполнительными и распорядительными органами ежегодного отчёта (общедоступной информации о результатах своей работы) за предыдущий год, исходя из своих основных направлений деятельности. В соответствии с проектом закона эта информация должна быть размещена в средствах массовой информации и (или) на интернет-сайтах не позднее 1 марта года, следующего за отчетным. Представляется, что более логичным было бы установление прямой обязанности размещения данной информации непосредственно на официальном сайте государственного органа.

Отметим, что данный перечень основан на требованиях Указа № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» и почти дословно перенесён в проект Закона из принятого в развитие Указа № 60 постановлением Совета Министров № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций», не вносит новых требований к информации, размещаемой на официальных сайтах и не повышает стандарты доступа к информации, находящейся в ведении государственных органов.

Посещение открытых заседаний

4

Ещё одним новым способом распространения и (или) предоставления общедоступной информации о деятельности государственных органов, в соответствии с проектом Закона, является проведение открытых заседаний, на которых обеспечивается возможность присутствия физических лиц, их представителей, представителей юридических лиц. Статья 222 устанавливает, что, кроме случаев обсуждения вопросов, содержащих информацию, предоставление и (или) распространение которой ограничено, заседания коллегий республиканских органов государственного управления, подчиненных Правительству Республики Беларусь, заседания местных исполнительных и распорядительных органов проводятся в форме открытых заседаний.

Информация о дате, времени и месте проведения открытого заседания, о предполагаемой повестке такого заседания размещается государственными органами на своих интернет-сайтах и (или) в средствах массовой информации, а также в этих органах в доступных для обозрения местах, как

правило, не позднее, чем за пять календарных дней до дня проведения открытого заседания. Единственным основанием для доступа на открытое заседание является наличие документа, удостоверяющего личность физического лица, представителя юридического лица, кроме тех случаев, когда государственным органом была организована предварительная запись на открытое заседание. Присутствующие на открытом заседании, с согласия должностного лица, проводящего заседание, вправе делать записи, а также проводить фотосъемку, аудио- и видеозапись.
Очевидно, что принятие данных норм может стать серьёзным шагом в обеспечении большей информационной открытости в деятельности государства и его органов.

Защита персональных данных

При разработке новой редакции Закона экспертами ожидалось большее внимание к области реализации права на неприкосновенность частной жизни и защиты персональных данных. Это, в первую очередь, выделение вопроса защиты персональных данных в отдельный закон (либо хотя бы отдельную проработанную главу существующего Закона), в том числе развитие законодательных терминов и определений в данной сфере, приведение норм Закона в соответствие с международными стандартами, и в первую очередь со стандартами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

Однако даже после принятия новой редакции Закона на основании анализируемого проекта проблема защиты персональных данных фактически остаётся нерешенной. В качестве подтверждения можно привести в пример нарушения права на частную жизнь и утечки персональных данных граждан. К сожалению, законодатель на данный момент ограничился лишь уточнением, что согласие на сбор, обработку, хранение информации о частной жизни физического лица и персональных данных должно быть получено в письменной форме (ст. 18 Проекта). Более никаких планов по дополнительному обеспечению защиты персональных данных, подвергающихся автоматической обработке, в Беларуси не предусматривается.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Изменения в Закон являются достаточно косметическими и не решают проблем существующих в данной сфере отношений.

Как говорилось выше, наибольшим разочарованием экспертов является отсутствие внимания законодателя к нерешенной проблеме защиты персональных данных, невосприятие подходов и принципов, изложенных в базовом законодательстве Совета Европы, а также подходов, используемых в соседних странах – Российской Федерации и Украине. Отметим, что отсутствие качественного законодательного регулирования порядка сбора, хранения, обработки и передачи персональных данных в первую очередь умаляет правовой статус обычных граждан, как в части соблюдения и гарантий права на частную жизнь, так и при использовании электронных сервисов – при покупке и заказе товаров и услуг, получении рассылок, направлении запросов.

Отмечая положительные изменения по расширению возможностей доступа к информации в виде участия в открытых заседаниях государственных органов, нельзя не обратить внимание на тот факт, что Законом не установлены четкие сроки информирования общественности о таких заседаниях, что в целом исключает ответственность органа за надлежащее информирование, а также практически неограниченные возможности должностного лица, проводящего заседание, по разрешению фиксации происходящего. Аналогичные претензии можно предъявить и к полномочиям руководителя государственного органа либо иного лица по предоставлению общедоступной информации, указанной в ст.21 Закона.

При этом не установлена обязанность мотивировать отказ каким-либо образом, не установлены четкие критерии, на основании которых может быть отказано в предоставлении информации либо в фиксации происходящего на открытом заседании, что может негативно влиять на практику применения Закона, особенно относительно острых проблем, привлекающих пристальное внимание общественности.

Установление нормы о возможности непредоставления общедоступной информации в случаях, если запрос направлен на выработку правовой позиции по запросу, проведении анализа деятельности государственного органа или проведении иной аналитической работы, непосредственно не связанной с защитой прав и законных интересов лица, направившего запрос, представляется в целом противоречащим европейской практике, которая допускает предоставление подобной информации, например, негосударственным организациям, действующим в общественном интересе, так называемым social watchdogs. Данная норма также может ограничить возможности влияния общественности на принятие общественно значимых решений.

Несмотря на введенную обязанность размещения определенной информации на интернет-сайтах государственных органов, в случае если запрашиваемая информация опубликована в официальных периодических печатных изданиях, средствах массовой информации или размещена в открытом доступе в глобальной компьютерной сети Интернет, у государственного органа отсутствует обязанность давать в ответе на запрос ссылку на такую информацию при формулировании отказа. Это также может быть основанием для манипулирования информацией и предоставления в определенных ситуациях так называемых пустых «отписок».

Также при обсуждении проекта Закона важно понимать, что в этой сфере в Беларуси много зависит от практики применения норм законодательства. Для большего обеспечения прав и законных интересов граждан, общественных организаций необходим общественный контроль как на стадии принятия Закона, так и практики его применения. Одной из важных форм контроля также может стать мониторинг интернет-сайтов государственных органов, направление запросов с целью мониторинга выполнения норм законодательства о доступе к информации, общественное давление для дальнейших изменений в сфере защиты персональных данных.

ТАК ЛИ БЕЗОПАСЕН SKYPE? 5 ЗАПРОСОВ О ВЫДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 35 АККАУНТОВ SKYPE ИЗ БЕЛАРУСИ

В блоге компании Майкрософт был опубликован ежегодный отчет по запросам к компании о выдаче персональных данных. Microsoft подчеркивает, что в соответствии с Global Human Rights Statement, а также в качестве члена Global Network Inintiative компания несет серьезную ответственность за соблюдение прав человека, принципов свободы высказывания и охраны частной жизни. В связи с этим Microsoft постоянно пересматривает свои внутренние политики, локальные нормативные акты и процессы менеджмента. Для сохранения прозрачности всех процедур компания ежегодно предоставляет общественности доступ к информации о запросах, которые в рамках уголовного преследования индивидуумов направляют в компанию правоохранительные органы различных государств.



В связи с отличиями правового регулирования данные по запросам информации пользователей продуктов компании Microsoft и Skype публикуются отдельно. Также стоит отметить, что несколько иной правовой режим применяется к запросам, поступающим в компанию из США и Ирландии, так как Компания находится под юрисдикцией этих государств и размещает там свои данные. То же самое касается и данных Skype, запрашиваемых правоохранительными органами Люксембурга, где находится штаб-квартира Skype Limited.

Компания Microsoft предоставляет SSL шифрование для продукции Microsoft и звонков Skype в зашифрованном виде на равной основе для всех пользователей, однако Компания обращает внимание, что безопасного на 100% способа связи не существует в любом случае. Например, при использовании Skype Out/In, маршрутизации при вызовах со смартфонов и мобильных устройств вызовы проходят через существующую телекоммуникационную сеть, со стороны которой и могут контролироваться. Кроме того, конечные точки доступа также могут являются уязвимыми для доступа третьих сторон (например, злоумышленников или спецслужб). Для обеспечения конфиденциальности связи следует принять меры по предотвращению заражения компьютеров и портативных устройств вредоносным программным обеспечением, а также осуществлять обновление программного оборудования только из надежных источников.

Microsoft отмечает, что уважая работу правоохранительных органов по раскрытию преступлений и поддержанию безопасности в их юрисдикциях, компания в то же время стремится уважать ущемляемые при осуществлении этой деятельности права человека и свободу слова.

В компанию ежегодно поступают запросы из различных стран. В отношении запросов, которые не отвечают принципам компании (так как некоторые пользователи программного обеспечения компании могут

находиться под контролем правительств или их права на свободу слова и распространение информации могут подавляться и контролироваться) производится отказ в выдаче данных. Согласно опубликованным данным в 2012 году беларусские спецслужбы пять раз обращались в компанию с запросами о 35 аккаунтах Skype. При этом компания выдала так называемые идентификаторы, затребованные в запросах. Сама переписка и прочие данные, которые относятся к содержанию переписки, голосовой и видеосвязи, выданы не были. Беларусь фигурирует только в списках запросов по Skype, по поводу данных пользователей остальных сервисов и служб Microsoft представители беларусских правоохранительных органов запросы не направляли.

Microsoft предоставляет правоохранительным органам данные исключительно на основании запросов судебных органов, а также субъектов, имеющих сходную юридическую силу, в отношении которых у Microsoft есть все основания полагать, что они подлинные. В случаях, когда нет достаточных оснований полагать, что запросы правоохранительных органов связаны с расследованиями уголовных дел, компания отказывает в предоставлении каких-либо данных о клиентах.

Выдаваемая информация, не содержащая переписки и иной личной информации пользователя, так называемая учетная информация пользователя или “non-contetnt data”, выглядит так:

Field	Value
Login	First.Last@xxxxxxx.com
PUID	0006BFFDA0FF8810
First Name	First
Last Name	Last
State	Washington
Zip	98052
Country	US
Timezone	America/Los_Angeles
Registered from IP	65.55.161.10
Date Registered {Pacific}	10/24/2007 1:05:18 PM
Gender	M
Age	1977
Last Login IP	64.4.1.11

Вот как компания Microsoft прокомментировала беларусским СМИ ситуацию с запросами из Беларуси: *«Юридическая служба Майкрософт внимательно изучила все пять запросов от судебных органов Беларуси, которые свидетельствовали о фактах расследований правоохранительными органами уголовных дел, например, связанных с хищениями с использованием украденных кредитных карт. Еще раз обращаем Ваше внимание, что ни в одном из случаев Skype не были предоставлены данные, выходящие за рамки учетных данных пользователя и касающихся содержания обмена данными».*

В русскоязычном сегменте Интернета в первом квартале 2013 г. широко обсуждался вопрос безопасности программы Skype для пользователей с точки зрения доступа спецслужб к персональным данным пользователей, возможности получения копий сообщений и прослушке звонков Skype.

В частности, на страницах российской газеты «Ведомости» гендиректор российской компании Group-IB утверждал, что спецслужбы «уже пару лет» могут не только прослушивать, но и определять местоположение пользователя Skype.

Выдержка из отчета компании Microsoft по запросам данных о пользователях Skype

Law Enforcement Requests Report

Skype

This data set is for Skype only.

	Calendar Year 2012			July 2012 - December 2012	
	Total # of Requests	Accounts/Identifiers Specified in Requests	Requests Resulting in Disclosure of Content	Accounts Specified in Requests Where Compliance Team Found No Data	Provided Guidance to Law Enforcement
TOTAL	4,713	15,409	0	2,847	501
Argentina	2	5	0	1	1
Armenia	2	6	0	3	0
Australia	195	424	0	118	8
Austria	10	18	0	0	4
Belarus	5	35	0	0	0
Belgium	39	165	0	45	3
Brazil	8	36	0	1	0

После того как Microsoft в мае 2011 года приобрела Skype, она снабдила клиента Skype технологией законного прослушивания, рассказывает исполнительный директор компании Peak Systems. Теперь любого абонента можно переключить на специальный режим, при котором ключи шифрования, которые раньше генерировались на телефоне или компьютере абонента, будут генерироваться на сервере. Получив доступ к серверу, можно прослушать разговор или прочитать переписку. Microsoft предоставляет возможность пользоваться этой технологией спецслужбам по всему миру, в том числе и российским, объясняет эксперт.

По словам специалистов информационной безопасности, доступ к переписке и разговорам в Skype российские спецслужбы не всегда получают по решению суда — иногда это происходит «просто по запросу». Считать, что прослушивание Skype представляет собой для российских правоохранительных органов непреодолимую проблему, нельзя, подтверждает сотрудник МВД. Официальные представители МВД и ФСБ Российской Федерации отказались от комментариев. Ранее глава российской Microsoft Николай Прянишников говорил, что Microsoft может раскрыть исходный код Skype Федеральной службе безопасности. Сам по себе код не позволил бы спецслужбам прослушивать разговоры, но при помощи его спецслужбы могли бы легче найти способ «дешифровки» информации.

Также известно, что в китайской версии Skype есть специальный механизм для отслеживания действий абонента. В китайский дистрибутив Skype встроен кейлоггер — специальная программа, фиксирующая действия пользователя на клавиатуре. Она проверяет тексты на содержание в них нежелательных слов и пересылает собранные логи спецслужбам. В перечень нежелательных слов предположительно могут входить следующие: Тяньаньмэнь (площадь, где в 1989 г. были подавлены протестные акции), Human Rights Watch, «Репортеры без границ», BBC News и др.

В белорусской судебной практике данные программы Skype были использованы в уголовном деле против участников Площади – в частности, в деле против Н. Статкевича, Д. Уса, А. Позняка, А. Класковского, А. Квяткевича, А. Грибкова и Д. Буланова в качестве доказательств имелся разговор Сергея Марцелева по скайпу. Однако в суде ходатайство о допросе Марцелева в качестве свидетеля в связи с указанным доказательством было отклонено. Имеются также и другие данные, позволяющие судить о том, что спецслужбы в Беларуси стремятся к получению и использованию данных пользователей программы Skype.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ УКАЗА №60: 5 ПРОТОКОЛОВ ЗА 2012 Г.

После введения в действие 1 июня 2010 г. Указа Президента Республики Беларусь №60 «О мерах по совершенствованию использования национального сегмента сети Интернет», предусматривающего ответственность за его нарушение, соответствующие изменения в КоАП Республики Беларусь были внесены только в конце 2011 г., и вступили в силу с 5 января 2012 г. Статьей 22.16 КоАП Республики Беларусь предусмотрены три состава административного правонарушения в этой сфере:

1 Осуществление деятельности по реализации товаров, выполнению работ, оказанию услуг на территории Республики Беларусь с использованием информационных сетей, систем и ресурсов, имеющих подключение к сети Интернет, не размещенных на территории Республики Беларусь и (или) не зарегистрированных в установленном порядке;

2 Нарушение требований законодательных актов по осуществлению идентификации абонентских устройств при оказании интернет-услуг и (или) пользователей интернет-услуг в пунктах коллективного пользования интернет-услугами, учету и хранению сведений об абонентских устройствах, персональных данных пользователей интернет-услуг, а также сведений об оказанных интернет-услугах;

3 Нарушение требований законодательства по ограничению доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами.

В качестве меры ответственности предусмотрены штрафы в размере до 30 базовых величин.

Доступ общественности к информации о привлечении субъектов к административной ответственности и указание конкретных составов по ст. 22.16 КоАП ограничен: эти данные не публикуются.



Тем не менее, **представитель ОАЦ В. Рябоволов** в интервью Еврорадио впервые озвучил данные о существующей практике привлечения субъектов:

«Мы поднимали административную практику за прошлый год, было всего 5 случаев составления административных протоколов за нарушения Указа№60, и это не было связано с интернет-кафе. Протоколы в основном составлялись налоговыми органами и были связаны с реализацией товаров, оказанием услуг, выполнением работ с использованием ресурсов, расположенных вне национального сегмента.

Хочу сказать, что многие нормы 60-го Указа приняты с целью защиты имущественных прав граждан. Например, человек покупает некачественный сотовый телефон и пытается предъявить претензии, но найти продавца невозможно. Так появилась норма, которая обязывает реализовывать товары, работы и услуги только на ресурсах, которые размещены на территории Беларуси. Но практика такова, что немного нарушений. Это плохо или хорошо? На мой взгляд, хорошо. Были выработаны понятные для всех правила и система дисциплинировалась».

О ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНОГО ЦЕНТРА ОБМЕНА ТРАФИКОМ (НЦОТ)

Указом Президента Республики Беларусь от 30.09.2010 №515 «О некоторых мерах по развитию сети передачи данных в Республике Беларусь» было утверждено создать единой республиканскую сеть передачи данных (далее - ЕРСПД), включив в ее состав сети передачи данных республиканских органов государственного управления, местных исполнительных и распорядительных органов, иных государственных органов и других государственных организаций, а также хозяйственных обществ, в отношении которых Республика Беларусь, либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами. В состав ЕРСПД не включаются сети передачи данных, предназначенные для обеспечения национальной безопасности, обороны и охраны правопорядка.

Для осуществления положений Указа к 1-му декабря 2010 г. было создано республиканское унитарное предприятие “Национальный центр обмена трафиком” (далее - НЦОТ).

Основными **задачами НЦОТ**, согласно законодательству, являются:

- обеспечение защиты от несанкционированного доступа к ЕРСПД и передаваемым по ней данным, пропуска трафика, а также управление ЕРСПД и принятие мер по ее развитию;
- обеспечение взаимодействия сетей передачи данных, а также государственных органов и организаций, иных юридических лиц и индивидуальных предпринимателей при оказании услуг электросвязи с использованием ЕРСПД;
- обеспечение равных условий доступа государственным органам и организациям, иным юридическим лицам и индивидуальным предпринимателям к ЕРСПД;
- организация расчетов за присоединение сетей передачи данных к ЕРСПД и за оказанные услуги электросвязи с использованием ЕРСПД (в том числе утверждение прейскурантов и тарифов);
- осуществление технического контроля за пропуском международного трафика и присоединением к сетям электросвязи иностранных государств;
- создание центров обработки данных, информационных сетей, систем и ресурсов, точек присоединения к сетям электросвязи иностранных государств и обеспечение их функционирования.

Сети передачи данных государственных органов и организаций, иных юридических лиц и индивидуальных предпринимателей присоединяются к ЕРСПД через НЦОТ в установленном порядке на основании Положения о единой республиканской сети передачи данных, утвержденного Постановлением Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь от 27.12.2010 N 8/28.

Также только НЦОТ и РУП «Белтелеком» входят в перечень операторов электросвязи, имеющих право на пропуск международного трафика и присоединение к сетям электросвязи иностранных государств, что часто является веским основанием указания на монополию государства в сфере пропуска и продажи трафика национальным операторам интернет-услуг.

Представитель ОАЦ **В. Рябоволов** высказал свое мнение о деятельности НЦОТ и влиянии его создания на упразднение монополии Белтелекома:

«В своем выступлении в ОБСЕ я говорил, что есть ряд факторов, сдерживающих развитие ИТ-сферы в Беларуси. Один из них – это фактическая монополия Белтелекома. Сказать, что единственный, - это не так. С Белтелекомом связано много положительного. Исторически сложилось, что это крупнейший национальный телеком. Многое, что сделано в республике, сделано благодаря участию Белтелекома, хотя это не единственный субъект на нашем рынке.

Основная часть сети, порядка 80 процентов, находится в собственности Белтелекома. Он – фактически владелец внешнего шлюза, весь трафик проходит через него, и потом он его реализует другим. Паритета цен достичь не получилось. Наверное, это в определенной степени проблема. Мы изучали мировую практику. Реформа национальных телекомов затронула многие страны Центральной и Восточной Европы. Мы тут не первые, это сложившаяся практика. Предполагаю, создание нормальной конкурентной среды будет условием для повышения эффективности деятельности всех участников рынка, в том числе и Белтелекома.

Создание НЦОТ вызвало определенные ожидания. Уже есть информационная среда, поэтому конкуренция начала реализовываться. В том числе, почувствовалось движение со стороны Белтелекома, и цены упали. Пока НЦОТ еще не реализует в полной мере свои функции. Для этого необходимо решение определенных задач: в первую очередь, создание инфраструктуры, техническое оснащение и, самое главное, значительные инвестиции. С этой целью создано предприятие “Беларусские облачные технологии”, одним из соучредителей которого является НЦОТ. В ближайшее время мы почувствуем конкретные результаты его деятельности.

Определение НЦОТа национальным оператором является первым шагом. Этот процесс будет продолжен. Наверное, реальная конкуренция предполагает наличие большего количества субъектов. Мы должны ответственно подходить к тому, что было создано в нашей стране. Все же Белтелеком — серьёзная организация, это социальный вопрос, там более 20 тысяч работников, сформированный коллектив, традиции... Создавая новое, необходимо учитывать то хорошее, что было сделано до нас».

«ЧЕРНЫЕ СПИСКИ» ИНТЕРНЕТ-САЙТОВ: КАК ЭТО РАБОТАЕТ?

Ограничение доступа к различным интернет-сайтам было введено Указом Президента Республики Беларусь от 01.02.2010 №60 «О мерах по совершенствованию использования национального сегмента сети Интернет».

Так, поставщики интернет-услуг оказывают услуги по ограничению доступа:

а) государственным органам и организациям, организациям образования, культуры, а также

б) по запросу иных пользователей интернет-услуг к информации, содержание которой направлено на:

- осуществление экстремистской деятельности;
- незаконный оборот оружия, боеприпасов, взрывных устройств, взрывчатых, радиоактивных, отравляющих, сильнодействующих, ядовитых, токсических веществ, наркотических средств, психотропных веществ, их прекурсоров и аналогов;
- содействие незаконной миграции и торговле людьми;
- распространение порнографических материалов;
- пропаганду насилия, жестокости и других деяний, запрещенных законодательством.

Законодательно порядок ограничения установлен постановлением Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь от 29.06.2010 N 4/11 “Об утверждении Положения о порядке ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами”. Поставщики интернет-услуг обеспечивают оказание услуг по ограничению доступа на основании списка ограниченного доступа, формируемого в установленном порядке Государственной инспекцией Республики Беларусь по электросвязи Министерства связи и информатизации (далее - РУП “БелГИЭ”) и списка ограниченного доступа, формируемого поставщиком интернет-услуг самостоятельно.

Список ограниченного доступа формируется РУП “БелГИЭ” на основании решений руководителей Комитета государственного контроля, Генеральной прокуратуры, ОАЦ, республиканских органов государственного управления (далее - уполномоченные государственные органы) о включении идентификаторов интернет-ресурса в список ограниченного доступа. Решения принимаются руководителями уполномоченных государственных органов в пределах их компетенции.

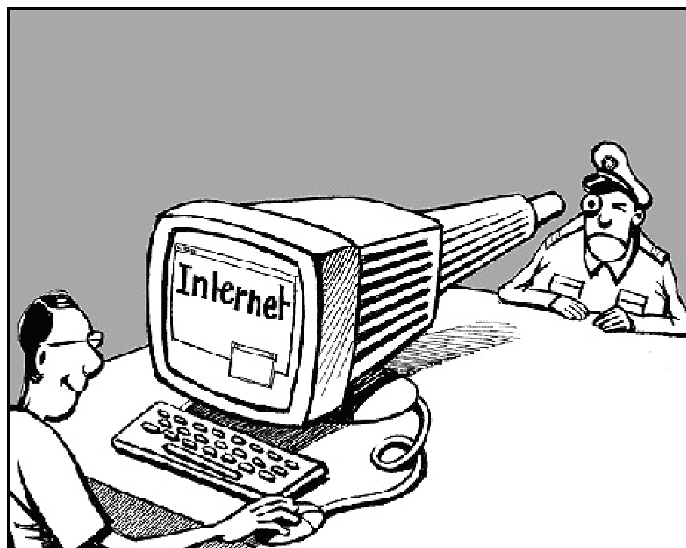
О принятом решении уполномоченным государственным органом в течение 3 рабочих дней направляется соответствующее уведомление:

- РУП “БелГИЭ”;
- владельцу (собственнику) интернет-ресурса, доступ к которому ограничивается, при условии нахождения данного интернет ресурса в национальном сегменте сети Интернет.

В уведомлении указываются:

- идентификаторы интернет-ресурса, доступ к которому подлежит ограничению;
- основания для ограничения доступа со ссылкой на норму законодательного акта, в соответствии с которой информация запрещена к распространению.

В случае отсутствия оснований для нахождения идентификаторов интернет-ресурса в списке ограниченного доступа уполномоченный государственный орган, принявший решение о включении их в данный список, принимает решение об исключении идентификаторов интернет-ресурса из списка ограниченного доступа. О принятом решении уполномоченным государственным органом в течение 3 рабочих дней также направляются соответствующие уведомления в РУП “БелГИЭ” и владельцу (собственнику) интернет-ресурса, доступ к которому ограничивается, при условии нахождения данного интернет-ресурса в национальном сегменте сети Интернет.



Юридические лица, их филиалы и представительства, а также индивидуальные предприниматели и граждане вправе обращаться в уполномоченные государственные органы с предложениями о формировании списка ограниченного доступа.

Список ограниченного доступа размещается на интернет-сайте РУП “БелГИЭ”. С ними можно ознакомиться по адресу: http://belgie.by/node/216 Доступ к списку для поставщиков интернет-услуг ограничен для обычных пользователей. При скачивании общедоступного списка – с сайта БелГИЭ скачивается пустой файл формата Excel.

Сведения, содержащиеся в списке ограниченного доступа с идентификаторами, определяющими интернет-ресурсы, зарегистрированные в национальном сегменте сети Интернет, носят общедоступный характер. Действия уполномоченных государственных органов, связанные с формированием списка ограниченного доступа, могут быть обжалованы в судебном порядке.

По вопросам “черных списков» сайтов представитель ОАЦ **В. Рябоволов** в публичном интервью пояснил следующее:

«Процедура внесения в список прописана. Ведение списков возложено на БелГИЭ, она формирует эти списки на основании мотивированных заключений, которые направляют уполномоченные госорганы. Насколько известно, большинство этих сайтов содержат порноматериалы и страницы экстремистского характера. Есть информация, что всего входит 119 ресурсов. Почему нельзя открыто посмотреть? Если бы они были в открытом доступе, то к ним был бы вызван дополнительный интерес. Зачем создавать им рекламу? Тем более, они же имеют ограниченный доступ только для госорганов, учебных заведений.

По поводу внесения в список заинтересованные лица могут обратиться в БелГИЭ и апелляция — это допустимый механизм, возможность апелляции должна быть. На конференции ОБСЕ выступал один из докладчиков на пленарном заседании, он говорил: должно быть прозрачно, мотивированно, и право на апелляцию. У нас процедура прозрачная, внесение в список мотивированное и есть право на апелляцию».

ОТМЕНА ОБЯЗАТЕЛЬНОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ПАСПОРТУ В ИНТЕРНЕТ-КАФЕ



На основании внесенных 22.12.2012 изменений в Положение о порядке работы компьютерных клубов и Интернет-кафе, утвержденного Постановлением Совета Министров Республики Беларусь от 10.02.2007 №175, **оказание услуг передачи данных или телематических услуг пользователю осуществляется после его идентификации, которая может производиться следующим образом:**

Конкретный способ идентификации определяется руководителем компьютерного клуба или Интернет-кафе или уполномоченным им лицом.

По данным ОАЦ не все интернет-кафе и клубы приветствовали нововведение, так как для оборудования организации дополнительными техническими средствами необходимо дополнительное финансирование. Однако на данный момент выбор способа фиксации осуществляется руководством организации, а не пользователем, в соответствии с указанным выше доступным перечнем способов идентификации.

После вступления в силу изменений журналисты «Еврорадио» проверили, как обстоят дела в минских интернет-кафе и общественных точках доступа: несмотря на нововведения ситуация никак не изменилась: для получения услуг доступа в интернет пользователю по-прежнему необходим паспорт. В некоторых случаях администрация была согласна на предъявления иных документов – таких как водительское удостоверение или читательский билет. Фото, -видео и смс-идентификация абонентов, несмотря на закрепление в законодательстве, на практике еще не применяется.

- по предъявляемому им документу, удостоверяющему личность,
- с использованием иных средств, позволяющих идентифицировать его личность (именная клубная карта, карта доступа и тому подобное),
- с использованием технических средств фото-, видеофиксации,
- иным программно-техническим способом (в том числе, SMS-сообщения), обеспечивающим сопоставление сетевых реквизитов пользователей с их персональными данными.

E-GOVERNMENT В БЕЛАРУСИ

В марте 2013 г. делегация из Южной Кореи посетила Минск по вопросам создания и работы электронного правительства. Делегация встречалась с рядом официальных лиц, и в том числе с помощником президента Всеволодом Янчевским. В Министерстве связи пояснили причины сотрудничества по этим направлениям именно с Южной Кореей: в рейтинге ООН они уже 2 года подряд лидеры среди 193 стран, поэтому позволяют себе учить других и передавать позитивный опыт.



Однако по мнению специалиста беларусского портала www.e-gov.by **Д. Гаврусика,** выбор корейского опыта для Беларуси не был случайным: корейская модель организации электронного правительства близка нашему государству. Это централизованный подход, при котором государство само определяет приоритеты, программу - и выполняет ее. При централизованном подходе государство само является и заказчиком, и частично исполнителем всех процедур. Другим примером можно считать Эстонию, в которой к процессу присоединяются частные компании, в том числе и в части финансирования. Бизнес участвует в процессе создания электронного правительства, а впоследствии имеет свою прибыль. Например, в государственном бюджете Республики Беларусь на создание и функционирование электронного правительства в 2013 г. выделено 11 миллиардов беларусских рублей.





По мнению руководителя проекта www.**e-belarus.org М. Дорошевича**, было бы разумно изучать мировой опыт, в том числе и корейский, но принимать оптимальные решения именно для Беларуси.

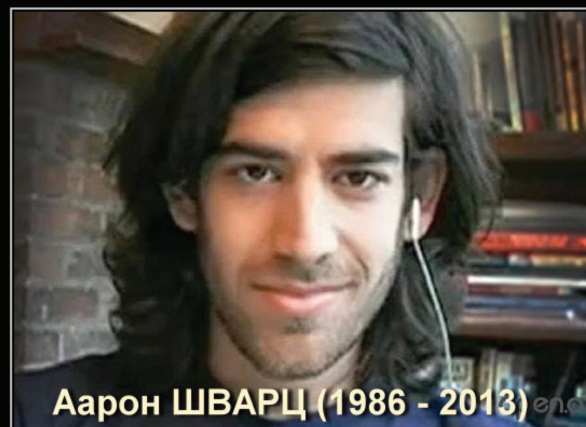
В рейтинге ООН по вопросам создания и функционирования электронных правительств на высоких позициях также находятся Нидерланды, Великобритания, Дания, США, Франция, Норвегия, Греция, Финляндия.

В Беларуси доступно около 100 электронных услуг, создана инфраструктура, государственные информационные ресурсы, центр электронных услуг, однако по мнению Дмитрия Гаврусика, не хватает фокуса именно на потребителях – отдельных гражданах. Так как информация про услуги не распространяется, мало потребителей знают о том, какие услуги сейчас доступны, а часть ссылок на портале госуслуг недоступны в принципе.

Согласно требованиям Еврокомиссии, в рамках электронного правительства должны действовать не менее 25 интернет-сервисов для граждан. Простое «копирование» сервисов, тем не менее, не представляет собой электронное правительство. Позитивным моментом в беларусском контексте назван открытый доступ через интернет к государственным кадастрам, реестрам, аукционам, государственным тендерам.

АМЕРИКАНСКИЙ ИНТЕРНЕТ-АКТИВИСТ ПОГИБ ЗА СВОБОДУ В ИНТЕРНЕТЕ

В январе 2013 года в Нью-Йорке покончил жизнь самоубийством один из самых известных в мире интернет-активистов в сфере борьбы за свободу информации Аарон Шварц.



Шварц родился в 1986 году, в 14 лет стал соавтором спецификации RSS 1.0, написал ряд книг, посвященных философии IT-пространства, в частности «Who Writes Wikipedia» и «HOWTO: Be More Productive», создал сервис Infogami, который впоследствии слился с популярным сайтом Reddit, а также был соучредителем движения против интернет-цензуры Demand Progress. В 2010-2011 академическом году, будучи сотрудником Центра этики Гарвардского университета, Шварц работал над исследованием политической коррупции: этому посвящен созданный им сайт watchdog.net. Еще одним направлением деятельности Шварца была работа на Open Library – это специальный некоммерческий онлайн-проект, где, по замыслу создателей, будут храниться все когда-либо опубликованные в электронном формате книги.

Причиной самоубийства активиста стали обвинения, выдвинутые против него должностными лицами прокуратуры штата Массачусетс и администрацией Массачусетского технологического института. Шварц был обвинен в мошенничестве, но виновным себя не признал, судебное разбирательство было назначено на апрель 2013 г. По предъявленным обвинениям из 13 пунктов (нарушение правил пиринговой сети, компьютерное мошенничество и незаконное скачивание контента с защищенного компьютера) ему грозило до 35 лет заключения.

Согласно официальному обвинению, Шварц похитил материалы, размещенные в онлайн-сервисе JSTOR, предлагавшем платный доступ к публикациям из научных журналов. По мнению прокурора, хакер планировал выложить их в одной из бесплатных файлообменных сетей.

JSTOR против Шварца иск не подавал: свободный гостевой доступ онлайн-сервиса предоставлялся работникам некоторых научных учреждений. Шварц, как штатный сотрудник Центра этики им. Сафры Гарвардского университета, имел на него право.

Позиция защиты Шварца была следующей:

Шварц входит в компьютерную сеть кампуса, которая никак не ограничивает сторонние подключения, подключается к сервису с архивом статей, который тоже открыт и доступен для пользователей сети и, написав несколько простеньких скриптов, выкачивает несколько гигабайт информации. То есть он не вламывается в закрытую сеть, не пытается получить доступ к закрытым данным, он просто скачивает больше, чем нужно ему самому в конкретный момент времени для того, чтобы сделать доступными широкому кругу лиц научные публикации, оплаченные общественными деньгами налогоплательщиков, но закрытые для подавляющего большинства тех, кто заплатил за них.

Однако, в связи с самоубийством Шварца, судебное разбирательство не состоится.

В знак протеста против действий прокуратуры и в память об Аароне Шварце в Интернете началась масштабная кампания. Ученые со всего мира публикуют в Facebook и Твиттере ссылки на файлы с защищенными авторским правом научными документами, а JSTOR объявил, что в ближайшее время в свободном доступе будут выложены более 4,5 млн файлов. Хакеры из группы Anonymous атаковали сайт Массачусетского технологического института и вывесили на нем некролог в память об Аароне Шварце, а также атаковали сайт американской комиссии по назначению уголовных наказаний - одного из независимых агентств правительства США, ответственного за вынесение приговоров в федеральных судах страны.

Смерть Аарона Шварца будет иметь далеко идущие последствия. Существующая система копирайта вызывает все больше недовольства; необходимость пересмотра, переосмысления права на копирование и распространение информации становится все более явной: нет справедливости в том, чтобы следовать несправедливым законам. Сайт организации, выступающей за свободное распространение информации Electronic Frontier Foundation заявил, что Шварц был экстраординарным хакером и ярким общественным активистом: он сделал больше, чем кто бы то ни было в мире для превращения Интернета в свободную платформу, позволяющую людям делиться друг с другом знаниями и для его сохранения в этом качестве.

Центр правовой трансформации некоммерческая организация, целью деятельности которой является повышение правовой культуры, организация просветительской, аналитической и исследовательской деятельности в области права.

Lawtrend группа профессионалов, которые, совместно действуя правовыми, исследовательскими и просветительскими методами, добиваются свободной реализации и эффективной защиты прав и свобод человека.